Section 14  Factor Groups

We have seen that the cosets of a subgroup $H \leq G$ sometime form a group. Such a group is called a factor group.

As an example, consider the cosets of $H = \langle 4 \rangle = \{0, 4, 8\}$ in the group $\mathbb{Z}_8$.

\[
\begin{align*}
0 + H &= \{0, 4, 8\} \\
1 + H &= \{1, 5, 9\} \\
2 + H &= \{2, 6, 10\} \\
3 + H &= \{3, 7, 11\}
\end{align*}
\]

The multiplication table of $\mathbb{Z}_8$ breaks up into blocks of cosets:

\[
\begin{align*}
0 + H &\quad 1 + H &\quad 2 + H &\quad 3 + H \\
0 + H &\quad 0 + H &\quad 1 + H &\quad 2 + H &\quad 3 + H \\
1 + H &\quad 1 + H &\quad 2 + H &\quad 3 + H &\quad 0 + H \\
2 + H &\quad 2 + H &\quad 3 + H &\quad 0 + H &\quad 1 + H \\
3 + H &\quad 3 + H &\quad 0 + H &\quad 1 + H &\quad 2 + H \\
\end{align*}
\]

We are going to further explore this idea. We will need the following basic fact:

Suppose $H \leq G$. Then:

1. $aH = a'H \iff a = a'h$ for some $h \in H$
2. $Ha = Ha' \iff a = h'a'$ for some $h' \in H$
Not every subgroup \( H \leq G \) will give rise to a factor group. \( H \) has to be a very special kind of subgroup. It must be what's called a **normal subgroup**.

**Definition** A subgroup \( H \leq G \) is a **normal subgroup** if \( gH = Hg \) for every \( g \in G \).

**Theorem** Suppose \( H \) is a normal subgroup of \( G \). Let \( G/H = \{ aH \mid a \in G \} \) = set of cosets of \( H \). Then there is a binary operation on \( G/H \) defined as \((aH)(bH) = (ab)H\) and \( G/H \) is a group under this operation. \( G/H \) is called a **factor group**.

**Proof** First we must check that this operation makes sense. If \( aH = a'H \) and \( bH = b'H \), we must show \((aH)(bH) = (a'H)(b'H)\)

i.e. \( abH = a'b'H \)

i.e. \( ab = a'b' \) for \( h \in H \).

Now \( aH = a'H \) means \( a = a'h_0 \) for \( h_0 \in H \)
And \( bH = b'H \) means \( b = b'h_1 \) for \( h_1 \in H \)
And \( b'H = Hb' \) means \( b'h_2 = h_0b' \) for \( h_2 \in H \).

Then \( ab = a'h_0b'h_1 = a'b'h_2h_1 = a'b'h \) for \( h \in H \).

This means \((aH)(bH) = (a'H)(b'H)\)
So the operation is well-defined.
Now we check group axioms.

\[ G_1 \quad (aH)(bH) \cdot eH = (abH) \cdot eH \]
\[ = abcH \]
\[ = (aH)(bcH) \]
\[ = aH(bH)(cH) \]

\[ G_2 \quad \text{The coset } eH = H \text{ is the identity because} \]
\[ (eH)(aH) = eaH = aH = (aH)(eH) \]

\[ G_3 \quad \text{The inverse of } aH \text{ is } a^{-1}H \text{ because} \]
\[ (aH)(a^{-1}H) = aa^{-1}H = eH = (a^{-1}H)(aH). \]

In short, if \( H \) is normal, then \( G/H \) is a group.

Notice that if \( G \) is abelian, every subgroup \( H \) is normal, for then \( gH = Hg \).

Thus if \( H \leq G \) and \( G \) is abelian, then \( G/H \) is always a group.
Example $\mathbb{Z}_{12}/\langle 3 \rangle$

Here are the cosets of $\langle 3 \rangle$: $0+\langle 3 \rangle \sim \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \\ 11 \end{array}$

Thus $\mathbb{Z}_{12}/\langle 3 \rangle = \{0+\langle 3 \rangle, 1+\langle 3 \rangle, 2+\langle 3 \rangle\}$

Here is the multiplication table. Notice that

$\mathbb{Z}_{12}/\langle 3 \rangle \cong \mathbb{Z}_3$

\[\begin{array}{cccc}
0+\langle 3 \rangle & 1+\langle 3 \rangle & 2+\langle 3 \rangle \\
0+\langle 3 \rangle & 0+\langle 3 \rangle & 1+\langle 3 \rangle & 2+\langle 3 \rangle \\
1+\langle 3 \rangle & 1+\langle 3 \rangle & 2+\langle 3 \rangle & 0+\langle 3 \rangle \\
2+\langle 3 \rangle & 2+\langle 3 \rangle & 0+\langle 3 \rangle & 1+\langle 3 \rangle \\
\end{array}\]

Example $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle (2,0) \rangle$

Notice that $\langle (2,0) \rangle = \{(0,0), (2,0)\}$

Here are the cosets of $H = \langle (2,0) \rangle$:

Here is the multiplication table. Notice that

$(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle (2,0) \rangle \cong \mathbb{V}$
How does all this tie in with homomorphisms?

Well, if \( \varphi : G \rightarrow K \) is a homomorphism, then it turns out that \( H = \text{Ker}(\varphi) \) is a normal subgroup of \( G \).

**Theorem** If \( \varphi : G \rightarrow K \) then \( H = \text{Ker}(\varphi) \) is a normal subgroup.

**Proof**

We need to show \( aH = Ha \) for any \( a \in G \).

**Idea:** Show

1. \( aH = \{ x \in G \mid \varphi(x) = \varphi(a) \} \)
2. \( H_a = \{ x \in G \mid \varphi(x) = \varphi(a) \} \)

(Then \( aH = Ha \))